UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,101	02/17/2004	Duc Pham	AESN3017	9887

23488 7590 07/05/2006

GERALD B ROSENBERG
NEW TECH LAW
260 SHERIDAN AVENUE
SUITE 208
PALO ALTO, CA 94306-2009

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 07/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)	
Office Action Summary	10/780,101	PHAM ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/14/2006*.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on March 14, 2006. Claims 1-18 are currently pending consideration.

Response to Arguments

2. Applicant's arguments filed March 14, 2006 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Grimm et al. (U.S. Patent 6,317,868), does not teach a "program signature." This argument is not found persuasive. The CPA discloses the use of a security identifier, which was deemed analogous in the previous Office action by giving the broadest reasonable interpretation to the claim in light of the specification. For the purposes of examination, the term "program signature" was interpreted as an identifier, which is associated with a program for identification and authorization purposes. This functionality is deemed to be performed by the security identifier in the CPA which can be associated with an object's name in a given namespace, and this identifier is used when the enforcement service queries the policy service (column 35-41). Therefore it is deemed, based on the present claim language, that the security identifier of the CPA is analogous to the program signature in the application. Furthermore, the Applicant argues that the CPA does not teach "request context related data." This argument is not found persuasive. The CPA teaches that the enforcement service queries the security policy service with the security identifier of the subject and the security identifier of the software component (column 6 lines 43-57). This query is a request of authentication/authorization of a software component which is sent from the enforcement service to the security policy service. The Applicant argues that the CPA does not teach a security request being sent prior to the execution of a software component. This is not found persuasive. The CPA states that the modified software component invokes the enforcement service *before* the original component operation is executed (column 6 lines 15-20). The enforcement service then queries the security policy service to authorize the execution of the component. The Applicant further argues that the CPA does not teach "authentication data and access attributes." This argument is not found persuasive. The CPA discloses that in addition to authentication software components, the security policy service also authenticates users (column 5 lines 64-67). Furthermore, the security identifier not only provides data of whether or not the software component should be executed, but also if its subject to different policies (column 5 lines 53-63). Therefore, it is asserted that the CPA does teach "authentication data and access attributes."

In view of the above arguments, the rejection is respectfully maintained as given below for claims 1-18.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grimm et al. (U.S. Patent No. 6,317,868).

Regarding claim 1, Grimm discloses:

A security server system that securely qualifies the execution of programs within a community of networked host computer systems, said security server system comprising:

b) a processor coupled to said database and including a memory storing a control program and" ***a communications network interface***" (Figure 5, column 9 lines 14-27) coupleable to "***a community of one or more host computer systems***" (column 9 lines 15-18), said processor "***operative to execute said control program in response to execution requests***" (column 4 lines 23-61, wherein the control program responds to queries and sends the enforcement policy to the host computer) received via said communications network interface from identifiable host computer systems within said community, wherein a predetermined execution request received from a predetermined host computer system includes "***an identification of a program load request***" (column 6 lines 15-41, wherein the security identifier identifies a program to the enforcement service), "***request context related data***" (column 6 42-57), and "***a***

secure program signature" (column 6 lines 15-41, wherein the security identifier identifies a program to the enforcement service), execution of said control program providing for "***determination of an execution control value based on an evaluation of said predetermined execution request relative to said sets of pre-qualified program signatures and defined policy rules***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed), whereby return of said execution control value to said predetermined host computer system securely qualifies the execution of the program identified with said program load request.

Grimm does not explicitly disclose a database storing sets of pre-qualified program signatures and defined policy rules associating execution permission qualifiers with execution control values. However, Grimm discloses that a server can parse the received data and based on information gleaned from the software component using its security identifier (program signature), to determine the policies that should be applied to the software component such as if the software component should be allowed to be executed by the client (column 5, lines 13-51, column 6 lines 43-67). Based on this reasoning, it is obvious that the server of Grimm has to have access to stored security identifiers (program signatures) and a list of policies (policy rules) corresponding to the security identifiers (program signatures). It is well-known in the art that such information is stored in databases. Therefore, it would be obvious to one of ordinary skill in the art at the time of invention to use databases to store security identifiers

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Grimm discloses:

The security server system of claim 1 wherein each identifiable host computer within said community includes an local operating system, said security server system further comprising "***a module implemented on each identifiable host computer system***" (column 4 lines 35-45, wherein the modified software component has a module which invokes the enforcement service) within said community in combination with said local operating systems, said module, responsive to said program load request, being operative to generate said predetermined execution request, said module, responsive to "***an execution request response including said execution control value, being operative to permit or deny said program load request***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Grimm discloses:

The security server system of claim 2 wherein execution of said control program "***provides for the lookup of said secure program signature in said database to identify a resource reference that is evaluated with said predetermined execution request to determine said execution control value***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed (control value)).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Grimm discloses:

The security server system of claim 3 wherein said "***predetermined execution request includes authentication data and access attributes determined from said local operating system relative to said program load request***" (column 5 line 64 – column 6 line 5, wherein in addition to the security identifier (access attributes), authentication is also provided).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Grimm discloses:

The security server system of claim 4 wherein execution of said control program provides for the "***selection of a default resource reference on a failure of the lookup of said secure program signature in said database***" (column 6 lines 30-41, wherein a default security identifier can be used), said default resource reference being evaluated with said predetermined execution request to determine said execution control value.

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Grimm discloses:

The security server system of claim 5 wherein said execution control value provides "***a specification to permit or deny said program load request and wherein***

said specification to permit is selectively qualifiable to include predetermined execution limitations including first limitations on said program load request" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed (control value)).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Grimm discloses:

The security server system of claim 6 wherein said "***predetermined execution limitations include second limitations on the execution of the program identified with said program load request***" (column 6 lines 58-67, wherein the security policy service provides an access mode for the software based on the security identifier (signature), wherein the policy includes many different rules of operation (limitations)).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Grimm discloses:

The security server system of claim 7 wherein said "***module, responsive to said execution control value, is operative to implement said predetermined execution limitations***" (column 5 lines 42-51).

Regarding claim 9, Grimm discloses:

A security server system that securely controls load execution of programs on a host computer system, said security server system comprising:

a) "***a module installed as a component of a host computer system***" (column 4 lines 35-45, wherein the modified software component has a module which invokes the enforcement service), said "***module operative relative to an operating system executed by said host computer system to intercept system calls to load an execute program for execution***" (column 4 lines 35-45, wherein the modified software component has a module which invokes the enforcement service), said module further operative "***to generate a security request containing a predetermined load request, associated authentication data and access attributes and a target secure program signature of an executable program identified by said predetermined load request***" (column 6 lines 15-41, wherein the security identifier identifies a program to the enforcement service); and

b) a security server further including "***a control program operative to parse said policy rules relative to said security request***" (column 6 lines 58-67, wherein the enforcement service checks the security identifier (program signature) and applies policy rules to each security identifier) and "***generate a security request response reflective of a match between said security request and a corresponding one of said policy rules***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed).

Grimm does not explicitly disclose a database storing sets of pre-qualified program signatures and defined policy rules associating execution permission qualifiers with execution control values. However, Grimm discloses that a server can parse the received data and based on information gleaned from the software component using its security identifier (program signature), to determine the policies that should be applied to the software component such as if the software component should be allowed to be executed by the client (column 5, lines 13-51, column 6 lines 43-67). Based on this reasoning, it is obvious that the server of Grimm has to have access to stored security identifiers (program signatures) and a list of policies (policy rules) corresponding to the security identifiers (program signatures). It is well-known in the art that such information is stored in databases. Therefore, it would be obvious to one of ordinary skill in the art at the time of invention to use databases to store security identifiers

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Grimm discloses:

The security server system of claim 9 wherein said "***module is responsive to said security request response to enable completion of said predetermined load request by said operating system***" (column 5 lines 42-51).

Claim 11 is rejected as applied above in rejecting claim 10. Furthermore, Grimm discloses:

The security server system of claim 10 wherein said "***control program is operative to lookup said target secure program signature in said first database to obtain a resource reference***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed) wherein said control program is operative to lookup said predetermined load request, associated authentication data and access attributes, and said resource reference in said second database "***to identify an applicable set of policy rules, and wherein said control program is operative to generate said security request response based on said applicable set of policy rules***" " (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Grimm discloses:

The security server system of claim 11 wherein said "***applicable set of policy rules includes a default policy rule corresponding to a lookup failure of said target secure program signature in said first database***" (column 6 lines 30-41, wherein a default security identifier can be used), said default resource reference being evaluated with said predetermined execution request to determine said execution control value.

Claim 13 is rejected as applied above in rejecting claim 9. Furthermore, Grimm discloses:

The security server system of claim 9 wherein said "***module and security server are interconnected by a communications network through which said security request is transmitted***" (Figure 5, column 9 lines 14-27).

Regarding claim 14, Grimm discloses:

A method of securing the execution of programs on a host computer system comprising the steps of:

a) "***intercepting, on a host computer, a load request for the execution of a program***" (column 4 lines 35-45, wherein the modified software component has a module which invokes the enforcement service);

b) "***determining authorization data and access attributes associated with said load request***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed);

c) "***generating a secure signature for said program***" (column 5 lines 26-28, wherein the security identifier (signature) for the program is determined;

d) "***providing a security request***" (column 6 lines 15-41, wherein the security identifier identifies a program to the enforcement service), including an identification of said load request, said authorization data and access attributes and said secure signature, to a security server, wherein said security server, in secure isolation from said host computer system, "***evaluates said security request and returns a security request response***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed); and

e) "***selectively enabling performance of said load request dependent on said security request response***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed (control value)).

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Grimm discloses:

The method of claim 14 wherein said security server performs the steps of:

a) "***evaluating said security request to determine whether said secure signature matches any of a plurality of predetermined secure signatures maintained in a first database by said security server***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed) and "***whether said identification of said load request and said authorization data and access attributes match any of a plurality of policy rules maintained in a second database by said security server***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed based on the policy rules); and

b) "***generating said security request response dependent on said step of evaluating***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Grimm discloses:

The method of claim 15 wherein said security server further performs the step of "***parsing a policy rule identified by said step of evaluating to implement the policy***

operation identified by said policy rule" (column 6 lines 58-67, wherein the enforcement service checks the security identifier (program signature) and applies policy rules to each security identifier), wherein said step of generating said security request response is further dependent on said step of parsing.

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Grimm discloses:

The method of claim 16 wherein said step of "***generating identifies in said security request response a control directive having at least the possible values of deny, enable, and enable subject to limitations***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed and if is executed, is executed adhering to the policy rules).

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Grimm discloses:

The method of claim 17 wherein said step of "***selectively enabling performance includes the step of constraining execution of said program dependent on said control directive***" (column 6 lines 15-57, wherein the enforcement service provides a response to whether or not the code is allowed to be executed and if is executed, is executed adhering to the policy rules).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA
06/11/06

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100